Proceedings of the 5th International Conference on Inventive Research in Computing Applications (ICIRCA 2023)
IEEE Xplore Part Number: CFP23N67-ART; ISBN: 979-8-3503-2142-5

IoT based Anti Theft Controlling and Security System for ATM Machine

Jothish Kumar M
School of Information Technology and Engineering,
Vellore Institute of Technology,
Vellore, Tamil Nadu, India
jothishkumar.m@vit.ac.in

Ramakrishnan Raman
Symbiosis Institute of Business Management, Symbiosis International (Deemed University),
Pune, Maharashtra, India.
ramakrishnan_raman@rediffmail.com

S. Prabhakar
Department of Mathematics,
S.A Engineering College(Autonomous),
Chennai, Tamil Nadu, India
prabhakars@saec.ac.in

T. Bernatin
Department of Electronics and Communication Engineering
Sathyabama Institute of Science and Technology
Chennai, Tamil Nadu, India.
bernatin.etc@sathyabama.ac.in

2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) | 979-8-3503-2142-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICIRCA57980.2023.10220945

***Abstract*— Nowadays, people often withdraw money from Automated Teller Machines (ATMs). Every user receives a unique card and personal identification code to perform all transactions secretly and anonymously. Developing an ATM crime prevention system is crucial to avoid theft. The proposed solution uses an embedded system using a Raspberry Pi to process the real-time data collected by the vibration sensor. In this instance, robberies are detected using a vibration sensor that hears buzzer sounds and senses vibration. The sensor provides information to a police station through the Internet of Things, and the main doors corresponding to the ATM close on their own so that the thief cannot be escaped. An IoT transmits data to a Wi-Fi module through a cloud server, which displays it in real-time. The mechanism alerts the bank staff automatically when an ATM is misplaced. Also, the proposed system uses cameras since they help us find theft suspects.**

Keywords*— *IoT, Sensors, Theft controlling, Security system, Camera

I. INTRODUCTION

The banking industry is one of the most crucial aspects in the modern world. Many people utilize banking facilities for their business-related operations. An Automated Teller Machine (ATM) is a technological tool that allows users to access their bank accounts from any location without bank personnel's assistance. With ATMs, users can carry out several financial tasks, such as cash withdrawals and transfers [1]. It has been noted that there are more crimes involving ATMs, which calls for increased ATM security. Recent technology offers transaction security to recognize authorized users. This is only applicable for safe ATM transactions, though. Using solid or gas explosives, removing ATMs, or other methods to access safes are examples of physical damage tactics. ATMs aren't protected unless physical protective measures are set in place. To prevent these issues, a theft prevention system is available. Anti-theft systems can be implemented using machine-to-machine communications technology [2].

The amount of people breaking into ATMs and overwhelming the security is a common occurrence these days. The employees took it, and the ATM's cash was also accepted. Hence, preventing robberies is a crucial function of automated security systems [3]. Algorithms for detecting traffic signs and colors can be utilized to detect movement within the ATM for more precise and trustworthy management. To boost security and reduce annoyance, every physical assault on an ATM must be observed. The work being suggested intends to develop an embedded system that utilizes the IoT not only for monitoring but also to halt other anonymous actions or physical attacks on ATMs and secure the safety of the cash provided with human help [4].

A low-cost standalone system based on the ESP8266 low-cost Wi-Fi module and cloud processing is what the suggested system aims to accomplish. The automated theft detection and warning mechanism in the Automatic Tailor machine is what this technology is meant to provide, along with energy savings through automation. The technology begins transmitting notifications and promptly closes the ATM's door and shutters when any hazard is detected, such as shaking, banging, fire, or high frequency [5]. ATM security and safety can be increased reasonably using this method. Seeing events around us led to developing and implementing a security-based ATM security warning work. The design method that aids in catching criminals who attempt to steal ATMs will be examined in this research. By using this technique, ATM facilities can also erect a security barrier. If someone manages to force the ATM open or harm it, these sensors send out an alert [6]. With this technique, software for ATM security is produced. Several methods are utilized, such as sleep detection, to increase the effectiveness of eye movement detection. The sensor ADXL335 and DHT22 in a security and monitoring system can be more trustworthy for real-time monitoring. Identifying suspicious behavior and image sampling improve image processing for security and surveillance [7].

In this setup, only one person can use the ATM at anytime. Alarms have been installed to improve safety, and vibration sensors aid in detecting any tampering with her ATM. The system is built on his IoT and Global Positioning System (GPS) technologies. It includes cameras installed to offer real-time updates, buzzers notifying the control room, monitoring room officers shutting the gates to his ATM cabin, and injecting chloroform into the cabin to make it more robber-proof. An increased security-based ATM

monitoring system was created due to observation of the situations around us [8]. This application targets ATM robbery prevention by integrating advanced algorithms with the current technologies present in the culture. A connected sensor module monitors the machine's vibrations to identify any attempts at ATM robbery. For additional protection, there is also the Panic Button. The Global System for Mobile Communications (GSM) will transmit a high warning message with a buzzer sound to the closest police stations and banking authorities when the panic switch is engaged or when vibration is detected. The system processes real-time data gathered by sensors and emergency button modules using an integrated PIC controller [9].

II. Literature Review

Biometric technology has increased the security of cash withdrawals, and a GSM-based technology is now employed for the same goal [10]. Combining the two methods is a strategy used by specific systems. An ATM is an electromagnetic device that enables financial clients to carry out cash withdrawals, installment payments, money transfers, and account information requests whenever want to, without dealing directly with a bank person. Today, fraud, robberies, and other security issues regularly strike ATMs. Ingenious and strategic techniques are also used [11]. Some of them are harmful and damaging. This research aims to improve ATM monitoring using embedded systems and other cutting-edge methods. This work presented solutions such as Radio Frequency Identification (RFID) cards instead of ATM cards and IR sensors that detect user movements and switch on/off air conditioners and lights as the user moves about. It saves power in this way. The problem can be solved by a live threat detection technique that transmits real-time information to police and centers in the case of malicious or unauthorized access [12].

Security at ATMs has become a severe problem, practically and electronically. Artificial neural network-based fingerprint sensors have been used to assist consumers in accessing data and conducting transactions because it is so challenging to create a safe environment. The shutters locking systems stop the robber from running away. With the advent of computer vision, a brand-new framework for safety and surveillance can now be used [13]. To notify the control room or police station in case of an accident at the ATM booth, it offers GSM module communication technology. SMS and phone services will also be accessible. To increase security overall, additional sensors have been added. This proposal suggests a centralized private server to keep track of every ATM in the city. The technology offers up-to-the-minute data and updates that assist in strengthening ATM security. Real-time data collection, processing, and transmission to the control center are done. This idea provides three levels of ATM security, including a GPS, to increase the environment's security [14].

An SMS alerting authorized bank staff members is instantly issued when such a signal is discovered. A solenoid valve immediately locks the door and sprays it with a cold mist; a loud siren is sent off to alert potential thieves to an actual burglary. These activities are all carried out in unison. Although cameras have become one of the most crucial pieces of surveillance equipment for ATMs, their superior quality makes it challenging to follow and identify offenders during suspicious behavior. It used super-resolution methods to enhance camera quality and offer high-quality, low-resolution footage to avoid this [15].

III. Proposed System

The proposed system initiative is to provide a complete security solution to safeguard ATMs against theft, damage, and illegal entry. It combines many parts and features for the ATM's integrity, safety, and security of the monies it stores. The system can be created and put into place by industry best practices and the particular needs of the ATM operator. To defend the ATM from physical assaults, the system has more robust casings, locks that can't be picked, and anti-drilling features. These precautions are designed to fend off attempts at forcible entry and discourage illegal access. The system contains sensors to detect different security breaches and an alert system. These sensors could be doors, motion detectors, vibration, or tamper sensors.

To enable quick reaction to possible threats, the sensors, when activated, set off an alert and transmit real-time warnings to a central monitoring station or security personnel. Remote monitoring and administration capabilities are made possible by the suggested system. It performs remote access to and management of the security system and gets alerts or notifications to users. Secure network connections or cloud-based platforms can be used to access data from a distance. A platform for central security management that offers a thorough overview of the security standing of all linked ATMs. Using this platform, security staff can effectively administer and maintain the security system by monitoring, managing configurations, and reporting.

Effective ATM theft control technology should be separated into primary systems while designing. For the device's construction, there are both software and hardware design. The proposed approach will provide a powerful ATM burglary security mechanism. The news and issues that are happening in people's daily lives serve as the inspiration for the work. As ATM theft and burglary are currently quite widespread, there are working to find a solution. The proposed an intelligent ATM robbery security system for the ATM, starting with a sensor at the entrance to GSM technology inside the ATM, keeping the concept of maintaining simplicity in view.

The system's sensors are continuously being monitored to identify any burglary attempts. The controller knows when the sensors have been tripped and when safety measures are required. The controller then engages the alarm system via the driver to deter the burglary attempt. Locking the shutters, the controller turns on the lockdown motor, closes the door, and traps the offenders within. It can keep an eye on and manage electrical risks. IOT-enabled control operations. The Raspberry Pi's CPU analyses every piece of input data and controls the output devices following that data. Vibration and infrared sensors, for instance, are connected to the Raspberry Pi's input pins. The Raspberry Pi's input is connected to the camera. The output pins are connected to the GSM, GPS, DC motor, and buzzer devices. All sensor and output devices have a 5V applied voltage. With the use of IOT, all information is sent to the webpage. Figure 1 shows block diagram of the security system for the ATM.

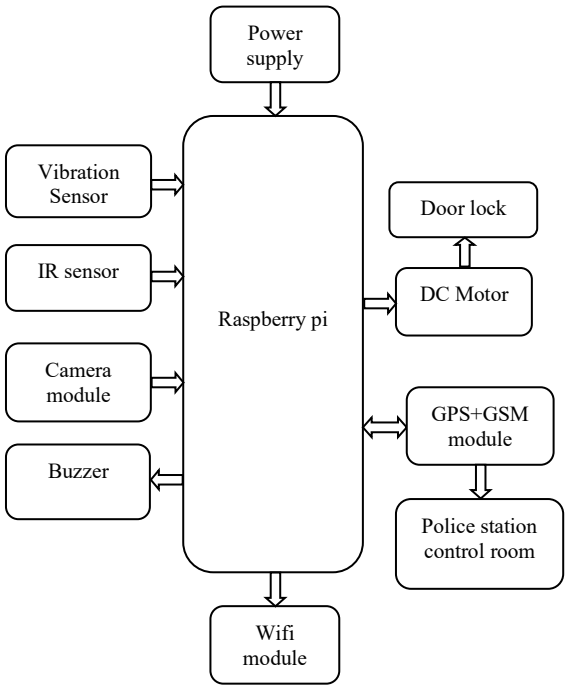

Fig. 1. Block diagram of the security system for ATM.

The ATM can be connected with a vibration sensor to track any unwanted physical tampering or attempted forceful access. The vibration sensor is often installed within the ATM shell or on essential access points, such as the door or card slot. It recognizes vibrations or motions when someone violently attempts to open or harm the ATM. When the vibration sensor notices these movements or vibrations, it sets off an alert or sends a signal to the security system. To warn security workers or law police of attempted theft, the alarm might be loud. The vibration sensor can also be connected to a camera system to record images or video of anybody trying to tamper with the ATM.

The presence of people close to the ATM, particularly around sensitive sections like the keypad or card slot, can be detected by an ATM security system using IR sensors. The IR sensor is a proximity sensor and can identify people approaching or standing near the ATM. By carefully arranging IR sensors around the ATM, the system can detect suspicious behavior, such as loitering or attempts to install cameras or skimming devices to steal card information. An alert to security staff, the activation of extra surveillance cameras, or the display of a warning message on the ATM screen can all be carried out when the IR sensor detects the presence of a person within a predetermined proximity zone.

The suggested framework controls ATM security against theft. An infrared sensor is used as an individual attempt to open a money locker using manual labor. When a sensor detects the movement of an item, the door will automatically close. Installed in the money locker, the IR sensor detects when the barrier passes and sends the information to the Raspberry Pi through the GPIO pins. The data gathered from the IR sensor and vibration sensor is operated by this framework using an embedded framework built on a Raspberry Pi. A buzzer will start to warn people if an incursion is found. Here, the door is opened and closed using a DC motor. In this instance, the dc motor is used to lock the door. The door opens every moment human moves in front of the infrared sensors. When a theft occurs, GSM is used to take images, and a message including the time of the crime is transmitted through GSM to a control center of the neighboring police station and also the relevant bank. A bank robbery's precise location was found using GPS. Also, a bell will go off to inform everyone of a theft. Figure 2 shows the workflow of the system.

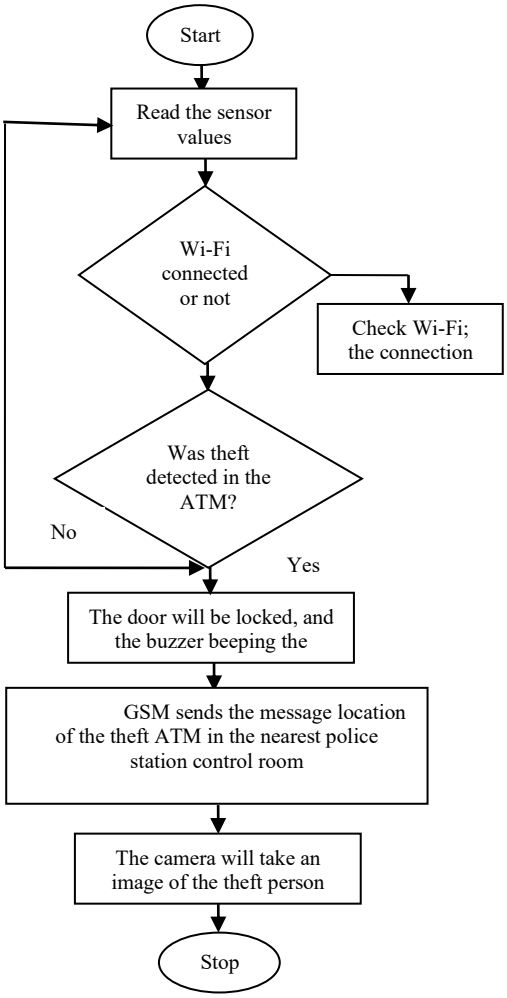

Fig. 2. Workflow of system

A. Raspberry pi

The Raspberry Pi Foundation's fourth single-board computer is the Raspberry Pi 4 Model B. The Raspberry Pi 4 Model B has a 1.5 GHz Broadcom BCM2711 quad-core ARM Cortex-A72 CPU. Compared to earlier models, it performs better. 2GB, 4GB, or 8GB LPDDR4 SDRAM is available for the Raspberry Pi 4 Model B. Multitasking and running memory-intensive apps are improved with more RAM. It supports OpenGL ES 3. x and has a VideoCore VI GPU for smooth graphics rendering and playback. The Raspberry Pi 4's micro HDMI connectors can drive two 4K displays. The Raspberry Pi 4 Model B has better connectivity than previous generations.

For peripherals, it has two USB 3.0 and two USB 2.0 connections. It includes Gigabit Ethernet, dual-band 802.11ac Wi-Fi, and Bluetooth 5.0 for wireless connectivity. The board stores data on a microSD card. A microSD card it install the operating system and store data. For external

storage devices, it includes two USB 3.0 connections. Users can attach sensors, actuators, and displays to the Raspberry Pi 4 Model B's 40 GPIO (General Purpose Input/Output) pins. A 5V USB-C power source powers the Raspberry Pi 4 Model B. The power needs are more significant than in prior versions; hence a power source with enough current is needed. The Raspberry Pi 4 Model B supports Raspbian (now Raspberry Pi OS), Ubuntu, and other Linux versions. Windows 10 IoT Core is supported. The Raspberry Pi 4's enhanced performance and power consumption need a heat sink or fan to avoid overheating.

IV. Result and Discussion

The proposed anti-theft controlling and security system for ATMs is a sophisticated electronic system offering increased security measures to prevent theft and unauthorized access. The design that has been presented incorporates different hardware and software components that collaborate to give an all-encompassing level of protection. To detect various effects on ATMs, the idea makes use of sensors. One of the outcomes is the effective operation of a Raspberry Pi-based Advance ATM anti-theft system. This technology could recognize the theft and alert the control room of the closest police station. An alarm SMS message is sent to the phone if there are vibrations within the ATM. The web server also displays the values that were obtained from the sensors. Thus, the policeman gets her GSM message via her SMS message on his Smartphone. Following the block diagram, all components were connected.

The software component of the system typically consists of a program that is developed in Python or another programming language compatible with Raspberry Pi and can be executed on it. The program analyses the data received from the sensors to identify any potentially harmful behavior and will issue a warning if one is required. It can also manage the power supply to the ATM and interact with a remote server to deliver real-time updates and alerts to the staff responsible for security.

When a theft occurs, a buzzer will signal a robbery, and a camera will take images while a dc motor closes the door and GSM transmits the message to the bank and the nearest police station. Also, to quickly resolve the problem, it could provide a nearby police station with a captured image of a theft.Figure 3 shows the circuit diagram of the system.

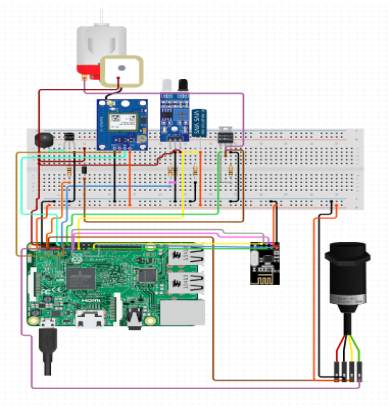

Fig. 3. Circuit diagram

Figure 4 shows the location view of the respective ATM in the GSM through the message. Captured images are stored in the database, and it can view them through web servers using IoT.

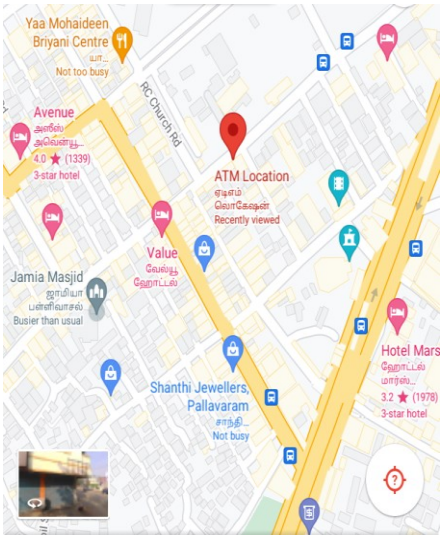

Fig. 4. The theft detection of ATM location

It has been developed by integrating features of all the hardware components and software used and tested. The proposed model, system for uses a mobile application. The sensors are utilized in ATM theft detection. A system's efficiency and success will be influenced by several variables, including how it was built, put into use, and maintained. Additionally, the outcomes can change based on how well each security measure works and how well it can handle possible threats and weaknesses. The technology aids in reducing the dangers connected to crimes using ATMs, such as physical assaults, card skimming, card entrapment, and unapproved access to cash. It is a deterrent, enabling prompt identification and reaction to security problems.

To analyze and improve the security system's performance, it might be helpful to work with security specialists, carry out risk assessments, and remain current on best practices in the field. To improve overall security and lower the risk of theft or unauthorized access to ATMs, regular testing, reviewing occurrences and actions, and integrating stakeholder input can help. A security operations center or central monitoring station should be able to integrate with the system so that alarms and notifications can be received there and handled quickly.

For ATMs to be as secure as possible, the security system has to adhere to all applicable industry norms and laws, such as those established by financial regulatory organizations. The technology reduces the amount of money lost due to theft and illegal access from ATMs. Rapid security issue detection and reaction can stop or lessen the effects of such occurrences, safeguarding the money and valuables kept within the ATMs.

The system's detection and identification of security threats have to be reliable. It has to be able to identify attempts at intrusion, tampering, or other suspicious behavior while keeping false positives to a minimum due to everyday events or ordinary ATM usage. Alarms can sound, security or police should be notified, and surveillance cameras should be turned on immediately if there is cause

for concern. To minimize danger and prevent ATM theft or damage, a prompt and trustworthy response is required. There has to be long-term effectiveness and dependability in the security system. It should be able to deal with avoidance or interference and robust against interference, being sensitive to false triggers from external factors such as electromagnetic interference or nearby vibrations.

The security solution should easily interact with the ATM infrastructure to minimize interruptions to ATM operations. It should not limit user use, compromise transaction security, or create technical issues that impair ATM availability. Sensor calibration, software upgrades, and hardware inspections should be performed regularly to maintain system performance. System faults should be addressed quickly with good technical help and troubleshooting. The security system's performance should be compared to its cost. It should provide a sufficient return on investment by efficiently safeguarding the ATM against theft, limiting losses, and decreasing possible liabilities.

Theft from ATMs can be reduced using a combination of physical and technological protections. The first step in preventing ATM theft is placing the machines in well-lit, safe settings. Alarms, tamper-evident design elements, and other security measures can detect and prevent thefts and other attempted interference. High-quality cameras in strategic locations for video surveillance capture critical evidence in the event of a theft. Safely anchoring ATMs and installing alarm systems provide further physical security. Skimming and tampering devices can only be detected with routine checks and maintenance. Users should be encouraged to be on alert for unusual behavior and report it. Finally, the security of the ATM system can be improved by giving bank staff comprehensive training on security standards and best practices.

ATMs in this system are protected by physical security features such as locked cases and tamper sensors to prevent theft and monitor for access. The ATM and its surroundings are constantly monitored with surveillance cameras, and the entrance door can be locked using a DC motor to prevent unwanted visitors from using the machine. These safeguards prevent burglaries or manipulation at the ATM by limiting the machine's mobility. Furthermore, alarm devices, such as a, can be included to offer audible alerts in the event of a security breach.

ATMs can be burglarized and equipped with several safety features that prevent theft. However, no security mechanism is flawless, and determined thieves can invent innovative means to overcome ATM security limitations. ATM burglaries usually include physical attacks, drilling, cutting, or explosives. ATMs include safe enclosures, sensors, and alarms to prevent such attacks.

When using an ATM, find a safe place, protect the user's PIN, be careful of surroundings, avoid strangers, frequently check user bank statements, beware of skimming devices, use reliable ATMs, and retain user receipts. These precautions reduce the danger of financial fraud and theft.

PIN authentication, encrypted data transfer, secure card readers, sensors and cameras for physical surveillance, secured lines of communication, transaction monitoring for identifying suspicious behavior, and routine maintenance and software upgrades are all standard features of modern ATMs. These protections ensure that user information is safe against burglary, fraud, and attack.

V. Conclusion

Advanced ATM anti-theft technology is developed in this research using IoT. ATM safety system with GSM and sensors is implemented. This initiative provides security for ATMs. A sensor detects vibrations whenever someone attempts to divert her ATM and sends a signal to the microprocessor. In response to the movement, the controller instructs the sprinkler to spray chloroform to put the burglar out of commission and the DC motor to shut the entrance to the ATM. The buzzer also operates concurrently. The controller simultaneously uses a GSM modem to transmit a message to the authorized police station control room. The prototype utilizes a vibration sensor to detect checking access movements, sounds an alarm in the event of an abnormality, and uses an actuator DC motor and integrated control to close the door while connecting to SMS messages. The location of the incident is communicated to a neighboring police station.

References

[1] M.M.E. Raj, and A. Julian, “Design and implementation of anti-theft ATM machine using embedded systems,” International Conference on Circuits, Power and Computing Technologies, pp. 1-5, 2015.

[2] P. More, and S. Markande, “Design and implementation of anti-theft module for ATM machine,” International Conference on Inventive Computation Technologies, vol. 3, pp. 1-4, 2016.

[3] H. Mahalakshmi, J. Nikhitha, and B. Varsha, “Implementing Anti-theft Systems for ATM and Vehicles,” Perspectives in Communication, Embedded-systems and Signal-processing , vol. 1, no. 12, pp. 196-2018.

[4] S. Gogineni, K. Marimuthu, and S.A. Sheik, “ IOT Based Centralized Bank Security System for Monitoring and Auto Arresting,” vol. 11, pp. 1-9, 2018.

[5] Y. Patil, P. Dusane, P. Rao, and P. Sutar, “Design and Implementation of Anti-theft System for ATM Machine using Internet of Things (IoT),” International Journal for Research in Applied Science and Engineering Technology, vol. 7, pp. 461-464, 2019.

[6] S. Usha, “Iot Based Anti-Theft Protection And Continuous Monitoring System For Atm,” Think India Journal, vol. 22, no .2, pp. 379-383, 2019.

[7] D. Ajay, G. Rangaraj, M. Sabarivasan, E. Yuvaraj, and N. Nithya, “Design and Implementation of Anti-Theft Module for Smart ATM Survillance System,” International Journal of Engineering Science, vol. 20731, pp.1-12, 2019.

[8] P. Arul, M. Meenakumari, N. Revathi, S. Jayaprakash, and S. Murugan, “Intelligent Power Control Models for the IOT Wearable Devices in BAN Networks,” 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, pp. 820-824, 2023.

[9] M. Zeyad, S. Ghosh, and S.M. Ahmed, “Design prototype of a smart household touch sensitive locker security system based on GSM technology,” International Journal of Power Electronics and Drive Systems, vol. 10, no. 4, pp. 1923-1931, 2019.

[10] R. Kumar, A. Sharan, V.K.S. Shah, Swapnil Shah. “Group Secret Key Generation for Wireless Network,” International Journal of MC Square Scientific Research, vol. 9, no. 1, pp. 260-273 , 2017.

[11] S. Ramyasri, and M. Mahalakshmi, “IOT Based Progressive Anti Theft ATM Security System,” IOP Conference Series: Materials Science and Engineering, IOP publishnig, vol. 981, no. 4, pp. 1-10, 2020.

[12] P.S. Patil, S.A. Lohkare, R.S. Patil, A.A. Tekade, and T.B. Kute, “Atm Surveillance, and Security Using Image Processing,” vol. 02, no. 07, pp. 844-848, 2020.

[13] A. Joy, "A systematic review comparing different security measures adopted in automated teller machine," Turkish Journal of Computer and Mathematics Education, vol. 12, no.13, pp. 388-393, 2021.

[14] V.S. Reddy, S. Kalli, H. Gebregziabher, and B.R. Babu, "Smart Door Lock to Avoid Robberies in ATM," In Journal of Physics: Conference Series, IOP Publishing, vol. 1964, no. 4, pp. 1-15, 2021.

[15] D. K. Verma, K. Singh, A. Srivastav, and V. Singh, "IOT based Smart Framework for ATM Security with Electricity Saver," vol. 10, no. 7, pp. 12-15, 2022